UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,447	04/27/2001	Timothy P. Farley	05456.105006	9081

20786 7590 11/08/2005

KING & SPALDING LLP
191 PEACHTREE STREET, N.E.
45TH FLOOR
ATLANTA, GA 30303-1763

EXAMINER	
GURSHMAN, GRIGORY	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,447	FARLEY ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-14 and 16-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-14 and 16-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/08/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

References submitted with the Information Disclosure Statement filed on 8/08/2005 have been considered. It is noted, however, that 49 pages of references were cited without an explanation as to how they came to Applicant's attention other that Applicant desires to not appear to be intentionally withholding prior art from the PTO.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

2. The term "substantially minimized" in claim 31 is a relative term, which renders the claim indefinite. The term "substantially minimized" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The degree to which a number of displayed events is minimized needs to be recited in the claim.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3-14, 16-31, 33-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka (U.S. Patent No. 6.453.345 B2) in view of Smaha (U.S. Patent No. 5.557.742).

5. Referring to the instant claims Trcka discloses a network security and surveillance system (see abstract and Fig. 3). Trcka teaches that a network security and surveillance system passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic. Raw data packets present on the network are continuously routed (with optional packet encryption) to a high-capacity data recorder to generate low-level recordings for archival purposes. The raw data packets are also optionally routed to one or more cyclic data recorders to generate temporary records that are used to automatically monitor the traffic in near-real-time. A set of analysis applications and other software routines allows authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events (see abstract and Fig. 3).

6. Referring to the independent claims 1, 14, 31, the limitation "receiving raw events from one or more data sources" is met by raw data packets present on the network (see abstract and Fig. 2). The limitation "classifying the raw events; storing the raw events" is met by filtering out packets based on pre-specified criteria (see 40 in Fig.1) and

recording processed packet stream on a storage medium (see 50 in Fig. 1). The limitation "assigning a ranking to each raw event" is met by pre-specified criteria for filtering (see Fig. 1 block 40). The limitation "identifying relationships between two or more raw events" is met by filtering traffic into "good" and "bad" packets as shown in Fig. 3. The analyses of raw events are performed in processing module 98 (Fig. 3).

7. Referring to the independent claims 18 and 22, the limitation "an event collector linked to the plurality of data sources" is met by archival data processing module (90 in Fig. 3). The limitation "a fusion engine linked to the event collector" is met by surveilance data processing module (94). The limitation "identifying relationships between two or more raw events generated by the data sources" is met by filter separating packets into "good" and "bad" ones (see unit 90 in Fig. 3). The limitation "a console linked to the event collector for displaying any output generated by the fusion engine" is met by GUI (104 in Fig. 3). Referring to claim 22, the limitation "a raw event classification database linked to the classifier" is met by media 80 (in Fig.3). The limitation "a context database linked to the context based risk-adjustment processor" is met by databases 82 and 82 linked to processing module 90 (see Fig.3). The limitation "a rule data base, for determining if relationships exist between two or more events" is met by traffic analyses databases (96 in Fig.3).

8. Trcka, however, does not teach determining if the two or more raw computer events are part of a larger computer attack. Referring to the instant claims, Smaha discloses a method and system for detecting intrusion into and misuse of data processing system (see abstract and Fig. 1). Smaha teaches that intrusion and misuse

detection system utilizes instructions for and steps of processing system inputs into events and processing the events with reference to a set of selectable misuses in a misuse engine to produce one or more misuse outputs. The system and method convert processing system generated inputs to events by establishing an event data structure that stores the event. The event data structure includes authentication information, subject information, and object information. Processing system audit trail records, system log file data, and system security state data are extracted from the processing system to form the event data structure. A signature data structure stores signatures that the misuse engine compares and matches to selectable misuses (see abstract). The "fusion engine" is met by misuse engine (30 in Fig. 1). The limitation "identifying relationships between two or more raw computer events with the fusion engine" is met by event data structure and the signature data structures. Determining if two or more computer events are part of the larger computer attack is met by comparing the data structures with signature structures (see Fig. 5a).

9. Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the network security and surveillance system of Trcka by adding the functionality for creating event data structures and comparing them with the signature data structures (i.e. determining if the events are part of the larger attack) as taught in Smaha. One of ordinary skill in the art would have been motivated to modify the network security and surveillance system of Trcka by adding the functionality for creating event data structures determining if the events are part of the

larger attack as taught in Smaha for comparing and matching to the known misuses (see column 3, lines 30-45).

10. Referring to the independent claims 1, 14, 31, Trcka shows displaying the event messages to the console (see GUI 104). Trcka, however, does not explicitly teach generating one or more correlation event messages.

11. Referring to claims 1, 14 and 31, Smaha teaches misuse output (42 in Fig. 1) and an index, which meets the limitation "correlation event message" .

Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the network security and surveillance system of Trcka by filtering the raw events and generating the correlation event message as taught in Smaha. One of ordinary skill in the art would have been motivated to modify the network security and surveillance system by filtering the raw events and generating the correlation event message as taught in Smaha for selecting the mechanism for loading the signature data structure (see Smaha , abstract).

12. Referring to the independent claim 14, the limitation "creating raw event storage areas based upon information received from a raw even classification database ans storing each event in an event storage area based upon an event type parameter" is met by storage areas 82 and 84 and the traffic analysis database 96 (see Fig.3 of Trcka). The limitation "comparing each raw event to the data contained in a context database" is met analysis applications running on the post-capture module coupled to traffic analysis database (see units 100, 98 and 96).

13. Referring to claims 31 and 35, the limitation "classifying the raw events" is met by separating raw data packets into "good" and "bad" ones (see Fig. 3). The limitation "displaying one or more ... messages on the console" is met by GUI (104 in Fig. 3).

14. Referring to claims 3 and 33, Trcka teaches that raw events are received in real time through the network card (88).

15. Referring to claims 5, 8 , 28 and 30, the limitation "comparing the event type parameter with the event type parameter of a list" is met by comparing parameters of captured raw data packet with the one ones stored in the traffic analysis data base (96).

16. Referring to claim 6, the limitation "assigning additional parameters to each raw event" is met by assigning "good" or "bad" status to the packets (see Fig.3, block 90).

17. Referring to claims 7, 16, 26 and 29, Smaha teaches sorting the events by type of misuse (i.e. context) prior to storing them.

18. Referring to claims 19 - 21, it is well known in the art have a detector comprising a chip and running in a kernel mode and fusion engine comprising software running on the computer. One of ordinary skill in the art would have been motivated to have a detector comprising a chip and running in a kernel mode and fusion engine comprising software running on the computer for enhanced scalability of the process.

19. Referring to claim 9, "associating each raw event with a rule which corresponds with a type parameter" is met by analysis applications (100).

20. Referring to claim 10, it is well known in the art to store event data in RAM. One of ordinary skill in the art would have been motivated to store raw events in RAM for utilizing high speed of access to RAM.

21. Referring to claims 17 and 25, it is well known in the art to have database comprising tables representing different categories of data. One of ordinary skill in the art would have been motivated to create a classification tables according to categories of raw event foe effective analysis of data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is (571)273-8300

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100